المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

الرئيسية سياسة

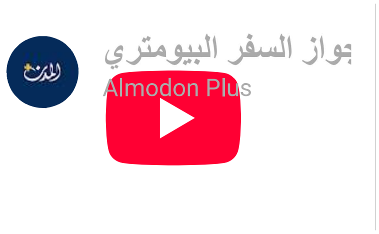
أفدح من جوازات سارية وباطلة: بيانات اللبنانيين المستباحة

لارا عاصي - بتول يزبك | الثلاثاء 2026/07/28

الدولة تطلب من مواطنيها تسليم أكثر بياناتهم ثباتًا وحساسية، ثم تكتفي بالقول إنها آمنة من دون أن تتيح لهم التحقق.

مشاركة عبر

حجم الخط



الأحداث المتدفقة على الساكن في هذه البقعة الجغرافيّة، لها طبقات من المعاني والتداعيات. إذ خلف كلّ أزمةٍ سياسيّة، أو توتّرٍ أمنيّ، أو حرب، أو تأزم اقتصاديّ، تمتدّ طبقاتٌ من التاريخ والمصالح والعلاقات الاجتماعيّة والرموز الثقافيّة الّتي تعيد تشكيل الحياة اليوميّة، وتمنح الحدث أبعادًا تتجاوز لحظته المباشرة. من هنا، تُطلق "المدن" سلسلة تحقيقات (multimedia) بعنوان: "فوق الأرض، تحت الأرض" للغوص في العوالم اللبنانيّة المختلفة، وتفكيك الأحداث الغامرة الّتي تنسحب من السّياسة والأمن والاقتصاد، إلى الثقافة والموضة والسوسيولوجيا والتحوّلات الحضريّة والظواهر اليومية. تنطلق السلسلة من الوقائع الظاهرة، ومن التفاصيل الّتي يعيشها الناس أو تمرّ أمامهم سريعًا، ثمّ تتتبّع ما تختزنه من قوى خفيّة، وشبكات مصالح، وصراعات على السّلطة والهوية والذاكرة.

تحاول هذه التحقيقات تجاوز الخبر العابر، وربط اليوميّ بالبُنيويّ، والفرديّ بالجماعيّ، والمرئيّ بما يجري خلفه. هي محاولة لقراءة لبنان من جهاته المتعدّدة: كما يظهر فوق الأرض، في الشارع والمؤسّسات والصور والخطابات، وكما يُصنع تحتها، في البنى العميقة التي تحرّك المجتمع وتعيد إنتاج أزماته وتحولاته.

تحاول هذه التحقيقات تجاوز الخبر العابر.

في هذه اللحظة، وأنت عالقٌ في الطابور الثالث، تنتظر أنّ ينادي العنصر الأمنيّ رقمك إيذانًا بالانتقال إلى طابورٍ آخر، يكون الضيق قد بلغ ذروته. خيطٌ رفيع من العرق يشقّ طريقه من أعلى ناصيتك إلى طرف عينك، والهواء الثقيل في الكوريدورات اللّولبيّة، والمكاتب الضيقة (الّتي ضربتها الرثاثة غالبًا) يزيد المشهد اختناقًا، ناهيك بالإرشادات الّتي تأتي على هيئة صراخٍ لا يُحتمل من عناصر مُرهَقة أصلاً. حولك أجسادٌ متلاصقة، ووجوهٌ أنهكها الانتظار، وأرقامٌ تُنادى ببطء، كأنّ الزمن نفسه عالقٌ في هذه الدائرة الحكوميّة.
إنّها بلا شكّ أعتى كوابيسك الكافكاويّة.

ستنظر إلى طابور المواطنين المحشورين في ممرّات مركز الأمن العام، وستقول في سرّك: هل الوثيقة الّتي جئت من أجلها "مهمّة إلى هذا الحدّ" كي تحتمل كلّ هذا؟
لكنّك ستبقى. لن تغادر بعد ساعةٍ أو ساعتين، أو حتّى أكثر، لأنّ ما تنتظره ليس ورقةً إداريّة عاديّة، ولا معاملةً يمكن تأجيلها بصورةٍ عرضيّة. إنّه جواز السفر، الوثيقة الّتي تختصر، بالنسبة إلى اللبنانيّ، حقّ التنقّل، وإمكان العمل، ولمّ شمل العائلة، وأحيانًا هي لصيقة فرصة النجاة من بلدٍ تضيق فيه الخيارات. هي مخرج طوارئ لا غنى عنها.

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

عليها، وقد دفعوا رسومها كاملة. لكنّ قرارًا إداريًّا مفاجئًا حوّلها، في لحظة، إلى وثائق محدودة القيمة، وحدّد الأوّل من تشرين الأوّل موعدًا نهائيًّا لاستبدالها.

ومنذ إعلان المديريّة العامّة للأمن العامّ وقف العمل بجوازات السفر اللّبنانيّة غير البيومتريّة من نموذج عام 2003، تحوّلت المراكز الإقليميّة إلى نقاط ضغطٍ جديدة. ويطاول القرار نحو 120 ألف جواز قديم، وفق تقديرات نقلتها وسائل إعلام عن مسؤولين في الأمن العام، بعضها لا يزال صالحًا حتّى عام 2027. لكنّ تاريخ الصلاحيّة المطبوع على الصفحة الأولى لم يعد كافيًا، إذ لن يُسمح، اعتبارًا من الأوّل من تشرين الأوّل 2026، لحامل هذا الجواز بمغادرة الأراضي اللبنانيّة بواسطته.

إلاّ أنّ الطوابير المُستجدّة والرسوم ليست سوى الطبقة الأولى من القصّة. فخلف الجواز البيومتريّ منظومةٌ كاملة تبدأ بالعقود والشركات التي تصنع الدفاتر والشرائح، وتمرّ بقواعد البيانات المركزيّة، ولا تنتهي عند بصمات الأصابع وصور الوجوه الّتي تجمعها الدولة من مواطنيها. وبين تبريرٍ أمنيّ عنوانه مكافحة التزوير، وأسئلةٍ قانونيّة عن مشروعيّة إبطال وثيقةٍ سارية، يفتح القرار ملفًّا مُهملاً ولكن أكثر خطورة: مَن يملك بيانات اللبنانيّين البيومتريّة؟ ومَن يستطيع الوصول إليها؟ ومَن يراقب الحارس؟

مَن يملك بيانات اللبنانيّين البيومتريّة؟

ماذا حدث؟

قرّرت المديريّة العامّة للأمن العام وقف العمل بجوازات السفر العاديّة غير البيومتريّة من نموذج عام 2003، وهي الجوازات التي تبدأ أرقامها عادةً بالحرفين "RL"، في مقابل الجوازات البيومتريّة الأحدث الّتي تبدأ أرقامها بالحرفين "LR". وبحسب القرار المعلن، يُطلب من حاملي الجوازات القديمة استبدالها قبل الأوّل من تشرين الأوّل، حتّى عندما لا تكون مدّة صلاحيّتها المدوّنة قد انتهت بعد. وبعد هذا التاريخ، لن يعود حامل الجواز القديم قادرًا على مغادرة لبنان بواسطته. تقول الرواية الرسميّة إنّ هذه الجوازات لم تعد تستوفي المواصفات المعتمدة في عددٍ متزايد من الدول، وإنّ الانتقال إلى النموذج البيومتريّ يهدف إلى الحدّ من التزوير ومواءمة معايير منظّمة الطيران المدنيّ الدوليّ، "الإيكاو".

من الناحية التقنيّة، لا خلاف على أنّ الجواز البيومتريّ أكثر تحصينًا من سابقه. فهو يحتوي على شريحةٍ إلكترونيّة تخزّن بيانات حامل الوثيقة، وتسمح بمطابقة صورة الوجه والمعلومات الشخصيّة مع البيانات الموجودة في النظام. لكنّ التطوّر التقنيّ لا يجيب عن السؤالين القانونيّ والماليّ: لماذا يُلغى

الأزمة الاقتصاديّة، خلال عامَي 2021 و2022، عجزت الدولة عن تأمين الكميّات المطلوبة من دفاتر الجوازات البيومتريّة. وتوقّفت منصّة المواعيد، وتراكمت الطلبات، وصار الحصول على جواز سفر مرتبطًا بالأولويّات والاستثناءات واللوائح الخاصّة. في تلك المرحلة، أعاد الأمن العام إصدار جوازات من نموذج عام 2003. لم يختر المواطن الجواز القديم، ولم يطلب وثيقةً أقلّ أمانًا أو صلاحيّة، بل عرضتها الإدارة نفسها بوصفها حلاًّ رسميًّا لأزمةٍ لم يكن المواطن طرفًا فيها. واليوم، تطلب منه الإدارة نفسها أن يعود إلى المركز، وأن يدفع من جديد.

هل القرار أمنيّ أم نتيجة نفاد المخزون؟

تقول مصادر "المدن" في وزارة الداخليّة والبلديّات إنّ وقف العمل بالجوازات القديمة جاء نتيجة الحاجة إلى توحيد وثائق السفر والانتقال الكامل إلى النموذج البيومتريّ.

لكنّ معلوماتٍ متقاطعة تشير إلى أنّ الأمن العام كان قد أبلغ بعثاتٍ لبنانيّة في الخارج بنفاد مخزون جوازات نموذج عام 2003. وهذه النقطة أساسيّة، لأنّها تغيّر طبيعة القرار. فإذا كان الوقف ناتجًا أساسًا من نفاد الدفاتر، يصبح الحديث عن المعايير الأمنيّة والدوليّة جزءًا من الرواية، لا الرواية كاملةً.

وحتّى الآن، لم يُنشر نصٌّ تفصيليّ يشرح ما إذا كان إبطال الجوازات السارية يستند إلى قرارٍ وزاريّ معلّل، أو إلى تعميمٍ إداريّ صادر عن الأمن العام، أو إلى واقعٍ تقنيّ فرضه نفاد المخزون. كذلك، لم تُنشر دراسةٌ تحدّد عدد المتضرّرين، ولا قيمة الرسوم التي سبق أن دفعوها، ولا الكلفة الإجماليّة التي سيتحمّلونها عند الاستبدال.

المصادر تُشير إلى أنّ هذه المسألة قد بدأت خلال لقاء الوزير أحمد الحجّار مع أبناء الجالية اللّبنانيّة في باريس، بحضور السفير اللّبنانيّ، حيث طرح الحاضرون مطلبين أساسيين تمثلا في إتاحة خدمة أخذ البصمة البيومترية في الخارج، وتخفيض رسوم جواز السفر البيومتريّ. وقد حمل الوزير الحجار هذين

دولة الكويت خلال الأيام الماضية، على أن تُعمم تباعًا على مختلف السفارات والقنصليات اللّبنانيّة حول العالم، وذلك بعد استكمال المديرية العامة للأمن العامّ جميع الإجراءات التقنيّة والإداريّة اللازمة، وتأمينها التغطية المالية المطلوبة، وذلك بالتنسيق أيضًا مع وزارة الخارجية والمغتربين. أما بالنسبة إلى تخفيض رسوم جواز السفر البيومتري، فقد تم ذلك بقرار مشترك عن وزيري المالية والخارجية والمغتربين، والذي أتاح خفض الرسوم، وفق ما أشارت المصادر.

شبكة التزوير: جوازٌ أصليّ وهويّةٌ مختلقة

لكن هل يُمكن فصل القرار الجديد عن ملفّ التزوير الذي نشأ خلال أزمة الجوازات بين عامَي 2021 و2022؟

تكشف معلوماتٌ قضائيّة عن شبكةٍ ضمّت ثلاثة عناصر من عديد الأمن العام، استغلّت الفوضى الإداريّة والضغط الهائل على مراكز إصدار الجوازات لتمرير طلباتٍ مبنيّة على مستندات وهويّات مزوّرة. (راجع "المدن")

لم يكن التزوير يجري من خلال صناعة دفترٍ مقلّد، فالجواز اللبنانيّ نفسه، بما يحتويه من خصائص أمنيّة وتقنيات طباعة معقّدة، يصعب تزويره ماديًّا. لذلك، بدأ الاحتيال من المرحلة الأولى، من خلال إخراج قيدٍ إفراديّ مزوّر، أو طلب جواز أعدّه مختار، أو بيانات شخصٍ غير موجود، أو هويّة شخصٍ ينتحل صفة آخر. كانت المعاملة تدخل المسار الإداريّ الرسميّ استنادًا إلى هذه الوثائق. وحين تصل إلى مرحلة الطباعة، يصدر جوازٌ حقيقيّ عن الدولة، لكنّه يحمل بياناتٍ مفبركة.

تمثّلت العقدة الأساسيّة في تمرير الطلبات عبر القيود المشدّدة التي فرضها الأمن العام خلال الأزمة. وهنا، بحسب المعلومات القضائيّة، برز دور ما عُرف بـ"الشعبة الخاصّة". في ذروة الأزمة، كان المدير العامّ للأمن العام يصدر لوائح استثنائيّة لإنجاز جوازات أشخاصٍ لديهم أسبابٌ عاجلة للسفر. وتفيد المعطيات بأنّ أحد العناصر استغلّ موقعه للوصول إلى هذه اللوائح وإضافة

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

على معاملات التجديد. والسبب تقنيّ، إذ إنّ الشخص الذي سبق أن حصل على جواز يملك أرشيفًا في قاعدة البيانات يتضمّن صورته وبصماته وبياناته، ولذلك تظهر التناقضات عند محاولة إدخال هويّةٍ جديدة باسمه. أمّا المتقدّم للمرّة الأولى، فيدخل النظام من دون سجلّ بيومتريّ سابق، ويصبح إخراج القيد أو الطلب المزوّر نقطة الانطلاق التي قد تسمح بإنشاء هويّةٍ تبدو جديدة داخل المنظومة.

أسفرت التحقيقات عن كشف إصدار أكثر من 60 جواز سفر بالطريقة الاحتياليّة. وعمّمت المديريّة العامّة للأمن العام أرقام هذه الجوازات وبياناتها على المطار والمعابر البرّيّة والبحريّة، بهدف توقيف أيّ شخصٍ يحاول استخدامها.

هل تبيع الدولة الخدمة مرّتين؟

يرى المحامي فاروق المغربي، الذي قابلته "المدن" في إطار هذا التحقيق، أنّ الخلل يبدأ من قرار الإدارة إبطال وثيقةٍ لا تزال سارية، من دون تحمّل كلفة الاستبدال أو توفير مرحلةٍ انتقاليّة عادلة.

ويقول إنّ كثيرًا من المواطنين حصلوا، خلال الأزمة، على جوازات غير بيومتريّة، ودفعوا رسومها كاملة، لأنّ الدولة لم تكن قادرةً على إصدار الجواز البيومتريّ. هؤلاء لم يرتكبوا خطأً، ولم يحصلوا على وثيقةٍ مخالفة للقانون، بل تقدّموا بطلباتٍ رسميّة، وأصدرت لهم الإدارة جوازاتٍ حدّدت صلاحيّتها بخمس سنوات.

ويضيف أنّ المنطق القانونيّ كان يقتضي استبدال الجوازات تلقائيًّا، أو إعفاء أصحابها من الرسوم، أو احتساب المدّة المتبقّية من صلاحيّتها ضمن ثمن الوثيقة الجديدة.

أمّا إجبار المواطن على دفع الرسم مرّتين، فيحوّل الإدارة، بحسب تعبيره، إلى جهةٍ تتصرّف كشركةٍ تجاريّة، لا كدولةٍ تتحمّل نتائج قراراتها.

يسأل المغربي: "ما الأساس القانونيّ الذي يسمح للدولة بأن تبيع المواطن الخدمة نفسها مرّتين؟".

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

والغاية من الرسم، والجهة التي تستفيد منه.

ويرى المحامي أنّ القرار قابلٌ للطعن أمام مجلس شورى الدولة، لأنّه يمسّ مراكز قانونيّة قائمة، ويُبطل وثائق أصدرتها الإدارة، ويفرض أعباءً إضافيّة على أصحابها.

لكنّه يشكّك في استعداد المواطنين لخوض هذا المسار. فصاحب الجواز يحتاج إلى السفر للعمل أو الدراسة أو العلاج، ولذلك يفضّل دفع الرسم على الدخول في نزاعٍ قضائيّ طويل.

يرى المحامي فاروق المغربي، أنّ الخلل يبدأ من قرار الإدارة إبطال وثيقةٍ لا تزال سارية.

الجواز في الداخل والخارج

تتفاوت كلفة جواز السفر بين لبنان والخارج تفاوتًا كبيرًا. ويدفع المغترب رسمًا أعلى، يُضاف إليه أحيانًا ثمن الانتقال إلى السفارة، وإرسال المستندات، وانتظار وصول الجواز من بيروت.

ولا تقتصر معاناة المغتربين على الرسوم، فلبنانيّون كثيرون يحملون جوازات من نموذج عام 2003، ويُقدَّر عدد حاملي هذا النموذج بنحو 120 ألفًا. وبعضهم لا يستطيع الحصول على جواز بيومتريّ جديد في السفارة ما لم يكن قد سجّل بصماته سابقًا في لبنان.

وقد عانى، خصوصًا، الأشخاص الذين تتراوح أعمارهم بين 16 و59 عامًا من شرط الحضور الشخصيّ إلى لبنان لأخذ البصمات عند استخراج جوازٍ بيومتريّ للمرّة الأولى.

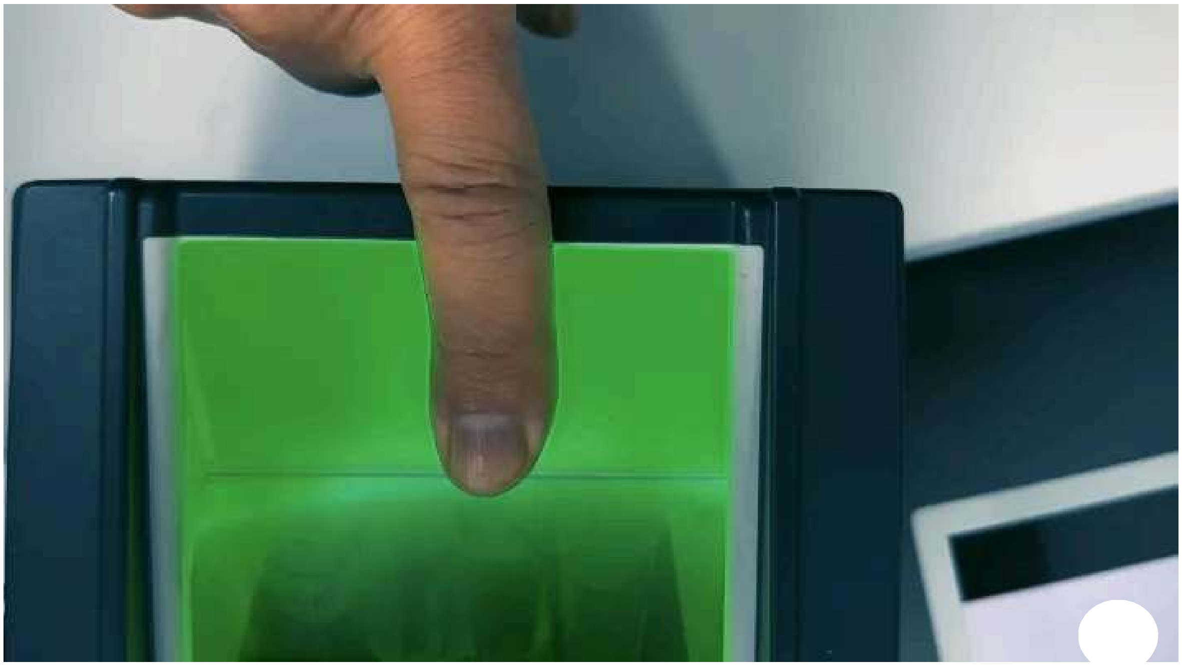
وبدأت الدولة أخيرًا إدخال محطّات البصمة إلى بعض السفارات، انطلاقًا من الكويت، على أن تُعمَّم الخدمة تدريجيًّا. لكنّ البطء في انتشارها يعني أنّ مغتربين قد يجدون أنفسهم بين جوازٍ قديم ستوقف الدولة العمل به، وخدمةٍ بيومتريّة لم تصل بعد إلى البعثة الأقرب إليهم.

ماذا يحتوي الجواز البيومتريّ؟

بدأ لبنان إصدار الجواز ذي الغلاف الكحليّ من نموذج عام 2003، ثمّ انتقل إلى الجواز البيومتريّ في آب 2016. ويحتوي الجواز البيومتريّ على شريحةٍ إلكترونيّة مدمجة في الدفتر، تُخزَّن فيها البيانات الشخصيّة الموجودة على صفحة الهويّة، إلى جانب صورة الوجه وبيانات بيومتريّة أخرى.

وبحسب المعلومات المنشورة عن المشروع اللبنانيّ، تجمع المنظومة صورة الوجه، وبصمات الأصابع العشر، وبصمات الكفّ، إضافةً إلى الاسم، وتاريخ الميلاد، والرقم الشخصيّ، وسائر المعلومات المطلوبة لإصدار الوثيقة.

ويتمثّل الهدف الأمنيّ في منع استخدام الجواز من شخصٍ آخر، وتعزيز قدرة أجهزة الحدود على مطابقة حامل الوثيقة مع البيانات المحفوظة في الشريحة والنظام المركزيّ. لكنّ هذه الفاعليّة الأمنيّة تأتي في مقابل جمع بياناتٍ لا يستطيع المواطن تغييرها إذا سُرقت. يمكن تغيير كلمة المرور، واستبدال البطاقة المصرفيّة، وإلغاء رقم الهاتف، أمّا بصمة الإصبع أو قالب الوجه فلا يمكن استبدالهما.



لا يعود السؤال محصورًا في قدرة الجواز على منع التزوير، بل يمتدّ إلى قدرة الدولة على حماية ما تجمعه.

لبنان ليس مخترَقًا فقط بل مكشوف

لمقاربة الجانب التقنيّ والحقوقيّ، قابلنا عبد قطايا، مدير برنامج الإعلام ومشروع حوكمة الإنترنت في منظّمة "سميكس"، وهي منظّمةٌ غير حكوميّة مقرّها بيروت، تُعنى بالحقوق الرقميّة، وحماية البيانات، وحرّيّة التعبيرعلى الإنترنت.

يرى قطايا أنّ لبنان يعاني تشتّتًا هائلاً في تخزين البيانات وإدارتها. فلا توجد بنيةٌ مركزيّة واضحة تضمّ جميع بيانات الدولة، بل تخزّن كلّ دائرةٍ ومؤسّسة ووزارة معلوماتها في مكانٍ مختلف. وقد تتوزّع بيانات الوزارة الواحدة بين مديريّاتٍ ومواقع وأنظمة لا ترتبط ببنية حماية موحّدة.

ويعزو ذلك إلى أنّ الدولة بدأت مسار الرقمنة من دون إدراك القيمة الاستراتيجيّة للبيانات، إذ تعاملت معها بوصفها ملفّاتٍ إداريّة، لا أصولاً

والنتيجة أنّ مؤسّسات الدولة رقمنت خدماتها وجمعت مزيدًا من المعلومات، من دون أن تبني، بالتوازي، منظومةً للحماية والمحاسبة.

وفي قراءته للقانون رقم 81، الصادر عام 2018 والمتعلّق بالمعاملات الإلكترونيّة والبيانات ذات الطابع الشخصيّ، يقول قطايا إنّ مسار إعداد القانون بدأ عام 2004، واستغرق 14 عامًا حتّى إقراره.

وخلال هذه المدّة، أُضيف إليه بند حماية البيانات، لكنّه بقي، بحسب قطايا، قاصرًا عن التعامل مع التطوّرات الحديثة.

ويعتبر أنّ من أبرز ثغراته عدم تصنيف البيانات الحسّاسة بصورةٍ واضحة، بما فيها البيانات الصحّيّة والبيومتريّة، وعدم إنشاء سلطةٍ مستقلّة قادرة على الرقابة والتحقيق وفرض العقوبات.

ويقول إنّ لجنة حماية البيانات، التي كان يُفترض أن تؤدّي دورًا رقابيًّا، لم تُنشأ بصورةٍ فعّالة، ما يعني أنّ الدولة والشركات تجمعان البيانات من دون وجود جهةٍ مستقلّة تدقّق في طريقة استخدامها.

ويختصر قطايا واقع الحماية بقوله: "لبنان ليس مخترَقًا فقط، بل مكشوف".

من رقم اللوحة إلى المنزل

لا يستند توصيف قطايا للبنان بأنّه "مكشوف" إلى احتمالٍ نظريّ، بل إلى سلسلةٍ من الوقائع التي تكشف أنّ تسرّب البيانات لم يعد حادثًا استثنائيًّا، بل تحوّل إلى خللٍ متكرّر في طريقة جمع المعلومات وحفظها وتبادلها.

> **تأتي بيانات هيئة إدارة السير والآليّات والمركبات في مقدّمة الأمثلة. فقاعدة البيانات التي تربط أرقام اللوحات بأسماء أصحاب المركبات وأرقام هواتفهم وعناوينهم لم تبقَ، بحسب قطايا، داخل حدود**

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

> والاضطرابات الأمنيّة، حين استُخدمت بيانات المركبات على الحواجز وفي عمليّات التدقيق. لكنّ توسيع دائرة الوصول إليها لم يترافق مع قواعد واضحة تحدّد مَن يحقّ له الاطّلاع، وكيف تُسجَّل عمليّات البحث، ومتى تُحذف البيانات أو تُمنع إعادة نسخها.

لاحقًا، خرجت هذه البيانات من نطاق الاستخدام الرسميّ، وصارت تُباع أو تُتداول عبر تطبيقاتٍ وقنواتٍ إلكترونيّة، من بينها روبوتات على تطبيق "تلغرام" وتطبيقات يمكن تنزيلها على الهواتف. ولا تكمن الخطورة في تداول نسخةٍ قديمة فحسب. إذ يؤكّد قطايا أنّ بعض قواعد البيانات المتاحة تتضمّن معلومات محدَّثة، ما يرجّح أنّ التسريب لم يكن واقعةً واحدة حدثت قبل سنوات وانتهت، بل إنّ جهةً ما ظلّت قادرةً على الوصول إلى السجلاّت الجديدة ونسخها أو بيعها.

إذا صحّ ذلك، فنحن لا نكون أمام أرشيفٍ سُرق مرّةً واحدة، بل أمام قناة تسريبٍ مستمرّة. والفارق بين الحالتين أساسيّ: ففي الحالة الأولى، تستطيع الدولة تغيير النظام، أو إلغاء الصلاحيّات القديمة، أو إخطار الأشخاص المتضرّرين. أمّا في الحالة الثانية، فهذا يعني أنّ الثغرة أو الصلاحيّة غير المشروعة بقيت مفتوحةً سنوات، من دون أن تنجح الرقابة الداخليّة أو القضاء أو الأجهزة الرقابيّة في تحديد مصدرها ووقفها.

ومن رقم لوحة سيّارةٍ واحدة، يمكن البدء ببناء ملفٍّ كامل عن صاحبها: اسمه، ورقم هاتفه، وعنوان سكنه، وربّما أفراد عائلته ومكان قيده. ويمكن بعد ذلك ربط هذه المعلومات بقوائم الشطب الانتخابيّة، أو ببيانات الاتصالات، أو بسجلاّتٍ تجاريّة ومصرفيّة وصحّيّة مسرّبة. عندها، لا تبقى كلّ قاعدة بياناتٍ منفصلةً عن الأخرى، بل تتحوّل السجلاّت المتفرّقة إلى خريطةٍ دقيقة لحياة الشخص وعلاقاته وتحركاته.

أو رسم شبكات العلاقات الاجتماعيّة والسياسيّة والمهنية، أو تسهيل استهداف شخصٍ بعينه.

ويتقاطع ذلك مع ما يشير إليه المحامي عن قوائم الشطب الانتخابيّة، التي تتضمّن أسماء الناخبين وتواريخ ميلادهم وأماكن قيدهم، وتنتقل إلى أحزابٍ وماكيناتٍ انتخابيّة من دون موافقةٍ فرديّة من أصحاب البيانات. كما يستحضر حادثةً تعود إلى نحو عشر سنوات، حين تسرّبت بياناتٌ كانت مجموعةً لدى أحد الأجهزة الأمنيّة إلى "الدارك ويب"، إثر خطأٍ تقنيّ نُسب إلى ضابط.

> **لا يحتاج الخطر دائمًا إلى مجموعة قرصنةٍ دوليّة أو هجومٍ تقنيّ بالغ التعقيد. قد يبدأ من موظّفٍ يملك صلاحيّات أوسع من حاجته الفعليّة، أو من كلمة مرورٍ مشتركة بين عدّة مستخدمين، أو جهازٍ غير محميّ، أو عقد صيانةٍ يسمح بالدخول عن بُعد، أو غياب نظامٍ يسجّل كلّ عمليّة بحثٍ ونسخٍ وتعديل.**

في هذه الحالات، يصبح السؤال عن "الاختراق" مضلّلاً أحيانًا، لأنّه يوحي بمهاجمٍ جاء من الخارج وكسر جدار الحماية. أمّا الواقع فقد يكون أبسط وأخطر: النظام نفسه يسمح لعددٍ كبير من الأشخاص بالدخول، من دون أثرٍ رقميّ واضح يبيّن مَن اطّلع على ماذا، ومتى، ولأيّ غرض.

اختراقات متكرّرة ولا جردة رسميّة

لا تقتصر السوابق على قاعدة بيانات السير. ففي المقابلة، أعادت محاوِرة قطايا التذكير باختراق منصّة حجز مواعيد جوازات السفر، ومنصّةٍ مرتبطة بهيئة

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

ويصعب، في ظلّ غياب بياناتٍ رسميّة تفصيليّة، وضع جميع هذه الوقائع في خانةٍ تقنيّة واحدة. فمصطلح "اختراق" قد يشمل هجومًا إلكترونيًّا من خارج النظام، أو تسرّبًا داخليًّا، أو قاعدة بياناتٍ تُركت متاحة على الإنترنت، أو نسخ موظّفٍ للمعلومات، أو حصول طرفٍ متعاقد على صلاحيّات لا تتناسب مع دوره.

لكنّ اختلاف الآليّات لا يلغي القاسم المشترك بينها: لم تنشر الدولة، في معظم الحالات، تقارير واضحة تبيّن طبيعة الحادث، والبيانات التي طاولها، وعدد الأشخاص المتضرّرين، وتاريخ اكتشافه، وموعد احتوائه، وما إذا كان المهاجم أو المسرّب لا يزال يملك نسخةً من المعلومات.

ومن بين التجارب الأكثر دلالةً منصّات جُمعت عبرها بيانات المواطنين خلال جائحة "كوفيد-19". ففي تلك المرحلة، ظهرت منصّاتٌ ونماذج متعدّدة مرتبطة بالتسجيل للقاحات، أو بتتبّع الحالات، أو بالحصول على مساعداتٍ وخدمات صحيّة واجتماعيّة. ويقول قطايا إنّ منظّمة "سميكس" أبدت في حينه تحفّظاتٍ على طريقة بناء بعض هذه المنصّات، وتواصلت مع الجهات الرسميّة والشركة التي عملت عليها.

لم تكن المشكلة في جمع البيانات الصحّيّة لغايةٍ عامّة فحسب، بل في تعدّد الجهات والمنصّات التي جمعتها، وعدم وضوح العلاقة بينها. فقد كانت وزارةٌ تنشئ منصّة، فيما تجمع جهةٌ أخرى بياناتٍ مشابهة في نظامٍ مختلف، من دون بنيةٍ موحّدة أو قواعد معلنة لتبادل المعلومات وحذفها بعد انتهاء الغاية منها.

وعندما انتهت مراحل من الجائحة أو تبدّلت برامج الدعم، لم تُبنَ الأنظمة الجديدة دائمًا على البنى السابقة، بل أُنشئت منصّات ونماذج جديدة. هكذا، تراكمت نسخٌ متعدّدة من بيانات المواطنين لدى وزاراتٍ ومؤسّسات وشركاتٍ متعاقدة، من دون أن يعرف صاحب البيانات أين بقيت معلوماته، ومَن احتفظ بها، وما إذا كانت حُذفت بعد انتهاء البرنامج.

الأمر نفسه ينسحب على منصّة المواعيد المرتبطة بجوازات السفر. فاختراق منصّةٍ لحجز الموعد لا يعني بالضرورة اختراق قاعدة البيانات البيومتريّة

جوازه أو معلوماتٍ إضافيّة بحسب الحقول التي كانت المنصّة تجمعها.

كما يمكن لهذه المعلومات أن تُستخدم في رسائل الاحتيال والتصيّد، إذ يصبح المهاجم قادرًا على مخاطبة المواطن بمعلوماتٍ صحيحة عن معاملته، وانتحال صفة الأمن العام أو موظّفٍ رسميّ، وطلب مبالغ ماليّة أو مستندات أو رموز دخول إضافيّة.

وتزداد حساسيّة الواقعة لأنّ منصّة المواعيد تمثّل البوّابة الخارجيّة لخدمةٍ ترتبط، في نهايتها، بواحدةٍ من أكثر قواعد بيانات الدولة حساسيّة. وحتى عندما يكون النظام الخارجيّ منفصلاً تقنيًّا عن النظام البيومتريّ الداخليّ، فإنّ اختراقه يطرح سؤالاً عن المعايير التي اعتُمدت عند اختياره واختباره، وعن وجود مراجعاتٍ أمنيّة مستقلّة قبل إطلاقه.

> لكنّ الدولة لم تنشر جردةً شاملة بهذه الحوادث. لا توجد، في متناول الجمهور، وثيقة تجمع الاختراقات والتسريبات التي طاولت الإدارات العامّة خلال السنوات العشر الماضية، وتصنّف أسبابها، وتحدّد البيانات المتضرّرة، وتبيّن ما إذا عولجت الثغرات.

وهذا ما يدفع قطايا إلى المطالبة بأن تبدأ الدولة من "جردة" كاملة: ما الأنظمة التي اختُرقت؟ ما البيانات التي خرجت؟ مَن كان يملك الصلاحيّة؟ هل تغيّرت كلمات المرور ومفاتيح التشفير؟ هل فُصلت الأنظمة المتضرّرة عن غيرها؟ وهل أُبلغ المواطنون الذين أصبحت معلوماتهم في أيدي جهاتٍ مجهولة؟

نظام حوكمةٍ لم يتغيّر.

مَن ينفّذ مشروع الجواز؟

أُسند تنفيذ مشروع الجواز البيومتريّ إلى شركة "إنكرييت"، التابعة لمجموعة "ريسورس غروب" التي يرأسها رجل الأعمال هشام عيتاني، بالتعاون مع شركة "جيمالتو"، التي كانت مسجّلةً في هولندا قبل أن تستحوذ عليها مجموعة "تاليس" الفرنسيّة عام 2019.

وبحسب المعلومات المتاحة، تولّت "إنكرييت" البرمجة وتطوير الأنظمة والحلول التقنيّة في لبنان، فيما تولّت "جيمالتو" تصنيع الدفاتر والشرائح والمكوّنات المرتبطة بالجواز الإلكترونيّ.

وتتداول تقارير صحافيّة رقمًا يقارب 140 مليون دولار بوصفه قيمة المشروع المموّل بمنحةٍ سعوديّة، لكنّ مصادر أخرى تحدّثت عن أرقامٍ أدنى. وهذا التضارب يستدعي العودة إلى العقد الأصليّ وملحقاته، بدل اعتماد رقمٍ غير منشور رسميًّا.

ولا تتعلّق أهمّيّة العقد بالقيمة الماليّة فقط، إذ يجب أن يحدّد النصّ ملكيّة البرمجيّات والشيفرة المصدريّة، وصلاحيّات الصيانة، وآليّات الدخول عن بُعد، والمتعهّدين الفرعيّين، ومدّة الاحتفاظ بالبيانات، ومسؤوليّة كلّ جهة عند حصول اختراقٍ أو تعطّل.

وتقول تقارير صحافيّة إنّ مالك "إنكرييت" محسوبٌ سياسيًّا على تيّار "المستقبل"، وإنّه نجل النائب السابق محمّد الأمين عيتاني.

لكنّ الصلة السياسيّة، في ذاتها، لا تثبت أنّ الشركة وصلت إلى البيانات أو سرّبتها. وما تفعله هو زيادة الحاجة إلى الشفافيّة، ونشر العقود، وإجراء تدقيقٍ مستقلّ، منعًا لتضارب المصالح أو الشبهات.

هل تملك الشركة قاعدة البيانات؟

وبحسب الرواية الرسميّة، تبقى قاعدة البيانات المركزيّة لدى المديريّة العامّة للأمن العام، فيما يقتصر دور الشركات على تزويد الدفاتر والشرائح والأنظمة التقنيّة.

لذلك، فإنّ الحديث عن "بيع البيانات" يحتاج إلى دليلٍ على نقلها، أو نسخها، أو منح الشركة صلاحيّة الوصول إليها. ولا يتوافر، حتّى الآن، دليلٌ علنيّ يثبت حصول ذلك.

لكنّ غياب الدليل على البيع لا يلغي الأسئلة. فالشركة التي تطوّر النظام أو تصونه قد تحتاج إلى صلاحيّات تقنيّة معيّنة. والسؤال هو: ما حدود هذه الصلاحيّات؟ وهل تشمل الدخول عن بُعد؟ وهل تستطيع الاطّلاع على سجّلاتٍ حقيقيّة أثناء الصيانة؟ ومَن يملك مفاتيح التشفير؟ وهل يراجع طرفٌ مستقلّ سجّلات الدخول؟

المشكلة ليست في إثبات سيناريو لم يقع، بل في غياب المعلومات التي تسمح للمواطن بالتأكّد من أنّه لا يستطيع الوقوع.

سابقة اختراق "جيمالتو"

في عام 2015، كشفت وثائق سرّبها إدوارد سنودن عن عمليّةٍ نُسبت إلى وكالة الأمن القوميّ الأميركيّة والاستخبارات البريطانيّة، استهدفت شبكات شركة "جيمالتو" ومفاتيح تشفير بطاقات الاتّصالات.

وقالت الشركة لاحقًا إنّها وجدت أسبابًا معقولة للاعتقاد بأنّ محاولة اختراق حصلت بالفعل، لكنّها لم تثبت حجم سرقة مفاتيح التشفير بالصورة التي وردت في بعض التقارير.

ولا يعني ذلك أنّ مشروع الجواز اللبنانيّ تعرّض للاختراق، ولا أنّ قاعدة بيانات الأمن العام مرتبطة بالشبكات التي استُهدفت حينها.

لكنّ السابقة تكشف أنّ الشركات الكبرى المتخصّصة في الأمن الرقميّ ليست منيعة، وأنّ الثقة باسم المورّد لا تكفي. فالحماية تحتاج إلى اختبارات اختراقٍ دوريّة، وفصلٍ بين الصلاحيّات، وتدقيقٍ مستقلّ، وخططٍ واضحة للاستجابة إلى الحوادث.

الظروف العاديّة، تُناقش حماية البيانات غالبًا بوصفها مسألة خصوصيّة وحقوق فرديّة: هل يجوز جمع المعلومة؟ ومَن يستطيع الاطّلاع عليها؟ وكم من الوقت يحقّ للجهة الاحتفاظ بها؟

لكنّ هذه الأسئلة تتبدّل عندما تصبح البيانات قابلةً للاستخدام في عمليّات المراقبة والاستهداف. فالمعلومة التي تبدو إداريّةً ومنفصلةً عن السياق الأمنيّ، مثل رقم لوحةٍ أو عنوان منزلٍ أو رقم هاتف، قد تتحوّل، عند ربطها بمصادر أخرى، إلى عنصرٍ داخل ملفّ استخباريّ أشمل.

خلال الحرب، ظهرت أسئلة متزايدة عن حجم البيانات التي تستطيع إسرائيل جمعها عن الأفراد والمناطق في لبنان، سواء عبر وسائل المراقبة الجويّة، أو اعتراض الاتصالات، أو تحليل المصادر المفتوحة، أو الوصول إلى قواعد بياناتٍ متداولة أو مسرّبة. ولا يتيح غياب المعلومات الرسميّة تحديد الحجم الدقيق لهذه البيانات، أو الفصل بين ما جُمع بوسائل تقنيّة مباشرة وما أُتيح من خلال تسريباتٍ سابقة.

لذلك، لا يمكن الجزم بأنّ قاعدةً لبنانيّة بعينها استُخدمت في عمليّة استهدافٍ محدّدة من دون دليلٍ تقنيّ أو تحقيقٍ مستقلّ. لكنّ الخطر لا يحتاج إلى إثبات استخدام كلّ قاعدة على حدة كي يصبح جدّيًا. فإتاحة بيانات المركبات والعناوين وأرقام الهواتف على نطاقٍ واسع تخفّض كلفة جمع المعلومات، وتتيح لأيّ جهةٍ تملك قدراتٍ تحليليّة أن تربطها بصور الأقمار الاصطناعيّة، وحركة الاتصالات، والحسابات الإلكترونيّة، وأنماط التنقّل.

ويشير قطايا إلى أنّ بيانات السير، مثلاً، يمكن أن تسمح بالانتقال من رقم اللوحة إلى اسم الشخص ورقم هاتفه وعنوانه، ثمّ ربط هذه العناصر بمعلوماتٍ أخرى وصولاً إلى الاستهداف، سواء بطائرةٍ مسيّرة أو بوسيلةٍ أخرى. ولا يقدّم هذا الكلام دليلاً على واقعةٍ بعينها بقدر ما يشرح المسار التقنيّ الذي يجعل البيانات المدنيّة المتاحة جزءًا محتملاً من منظومة الاستطلاع.

وتستخدم إسرائيل أنواعًا متعدّدة من الطائرات المسيّرة في الأجواء اللبنانيّة، تختلف وظائفها بين الاستطلاع والمراقبة وجمع الإشارات وتنفيذ الضربات.

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

هنا تظهر قيمة قواعد البيانات المجمّعة. فمن خلال دمج أرقام الهواتف بسجلّات المركبات والعناوين والعلاقات العائليّة أو المهنيّة، يمكن تضييق دائرة البحث، وتحديد المركبة التي يستخدمها شخصٌ ما، أو الأماكن التي يرجّح وجوده فيها. وكلّما كانت البيانات محدّثة وأكثر ترابطًا، ارتفعت قيمتها الاستخباريّة.

ولا يعني ذلك أنّ كلّ عمليّة اغتيال أو ضربة جويّة قامت على بياناتٍ مسرّبة من الدولة اللبنانيّة. فقد تُجمع المعلومات عبر مراقبة الاتصالات، أو العملاء، أو الصور الجويّة، أو وسائل التواصل الاجتماعيّ، أو تحليل الحركة الميدانيّة. لكنّ تسرّب قواعد البيانات يضيف مصدرًا آخر، ويجعل عمليّة التحقّق من الهويّة والمكان أسرع وأقلّ كلفة.

كما أنّ الحرب وسّعت حجم البيانات التي جمعتها الدولة والجهات الإغاثيّة داخل لبنان. فبرامج مساعدة النازحين والمتضرّرين قد تتطلّب أسماءً وأرقام هويّات وعناوين سكنٍ مؤقّتة وأرقام هواتف ومعلوماتٍ عن أفراد الأسرة والوضع الصحّيّ والاقتصاديّ. وتكون الحاجة إلى هذه البيانات مفهومةً لتوزيع المساعدات ومنع التكرار، لكنّ الاستعجال في إطلاق المنصّات قد يدفع إلى تجاوز تقييمات المخاطر، أو إلى منح شركاتٍ ومتعهّدين صلاحيّات واسعة.

قطايا: "لبنان ليس مخترَقًا فقط، بل مكشوف".

ويقول قطايا إنّ "سميكس" تابعت خلال الحرب طبيعة البيانات التي كانت تُجمع في لبنان، وحذّرت من الخروق المحتملة، وإنّ عددًا من المخاوف التي أُثيرت تحقّق لاحقًا. ولا يحدّد في المقابلة كلّ حادثةٍ على حدة، لكنّه يربط بين تكرار جمع المعلومات عبر منصّاتٍ مختلفة وبين غياب البنية الموحّدة للحماية والمساءلة.

وتكمن المفارقة في أنّ الأشخاص الأكثر حاجةً إلى المساعدة هم غالبًا الأكثر اضطرارًا إلى تقديم بياناتهم. فالنازح لا يملك دائمًا خيار رفض ملء النموذج إذا كانت المساعدة الغذائيّة أو بدل الإيواء مشروطين به. لكنّه لا يحصل، في المقابل، على معلوماتٍ واضحة عن الجهة التي ستخزّن بياناته، أو مدّة الاحتفاظ بها، أو الجهات التي ستتشاركها، أو الإجراءات التي ستُتّخذ إذا وقع اختراق.

وهنا تلتقي بيانات الحرب بالبيانات البيومتريّة. فالدولة التي لم تنشر بعد تقييمًا شاملاً لاختراقات منصّاتها السابقة تطلب اليوم من المواطن أن يسلّمها بصماته وصورة وجهه وقوالب بيومتريّة ثابتة. ولا يكفي، في بلدٍ يتعرّض للمراقبة والحرب السيبرانيّة والجويّة، أن تكون قاعدة البيانات محميّة من التزوير الداخليّ؛ يجب أن تكون مصمّمةً على افتراض أنّ جهاتٍ ذات قدرات تقنيّة واستخباريّة كبيرة ستحاول الوصول إليها.

مستقلّة، ومراقبة عمليّات البحث والنسخ، ووضع خططٍ لاستمرار العمل والاستجابة للحوادث في زمن الحرب.
فالأمن السيبرانيّ، في هذا السياق، لا يعود تفصيلاً تقنيًّا أو بندًا في عقد شركة. يصبح جزءًا من الأمن القوميّ، لأنّ قاعدة البيانات التي تُنشأ لتسهيل خدمةٍ مدنيّة قد تتحوّل، إذا خرجت من السيطرة، إلى أداةٍ تساعد على رسم المجتمع ومراقبته واستهداف أفراده.

حاجة تقنيّة

في ردّها على أسئلة التحقيق، وبصفتها الجهة الوصيّة على المديريّة العامّة للأمن العام، قدّمت مصادر في وزارة الداخليّة والبلديّات جملةً من الإيضاحات.
وبحسب المصدر، جاء قرار وقف العمل بالجوازات غير البيومتريّة بعدما اطّلع وزير الداخليّة أحمد الحجّار عليه من المدير العامّ للأمن العام، على قاعدة أنّ الجواز القديم لم يعد يستوفي المواصفات والمعايير المعتمدة في عددٍ كبير من الدول.
ويقول المصدر إنّ تحديد الأوّل من تشرين الأوّل موعدًا نهائيًّا يهدف إلى منح اللبنانيّين مهلةً كافية لإنجاز معاملات الاستبدال، لا إلى فرض وقفٍ فوريّ.
لكنّ الردّ لم يوضّح ما إذا كان القرار يستند إلى نصٍّ وزاريّ رسميّ منشور، أو إلى تعميمٍ صادر عن الأمن العام، أو إلى سببٍ تقنيّ يتعلّق بنفاد مخزون جوازات نموذج عام 2003. كما لم يحدّد الجهة التي تتحمّل مسؤوليّة الازدحام، أو سبب عدم إعفاء أصحاب الجوازات السارية من الرسوم.
ويربط مصدر وزارة الداخليّة إطلاق خدمة البصمة في الخارج بلقاءٍ جمع الوزير الحجّار بأبناء الجالية اللبنانيّة في باريس، حيث طُرح مطلبان: إتاحة أخذ البصمة البيومتريّة في السفارات بدل إلزام المغترب بالسفر إلى لبنان، وخفض رسم الجواز في الخارج.
وبحسب المصدر، نقل الوزير المطلبين إلى لبنان وعرضهما على رئيس الجمهوريّة، قبل أن يُتّخذ قرارٌ بخفض الرسوم، بالتنسيق مع وزيرَي الماليّة والخارجيّة والمغتربين.

> لكنّ جواب الوزارة لم يتضمّن الكلفة الفعليّة لإنتاج الجواز، ولا طريقة توزيع الرسوم بين الخزينة والأمن العام والبعثات والشركات المتعاقدة، ولا تفسيرًا واضحًا للفارق الذي يدفعه المغترب.

كيف تنتقل البيانات من السفارات؟

في شقّ حماية البيانات، يؤكّد المصدر أنّ محطّات استقبال الطلبات المركّبة في السفارات مطابقة لتلك المعتمدة في مراكز الأمن العام داخل لبنان.

ويقول إنّ هذه المحطّات تعمل بأنظمةٍ وبرامج خاصّة، ولا يستخدمها إلاّ الموظّفون المخوّلون، وهي مرتبطة بالنظام المركزيّ عبر شبكاتٍ آمنة.

وبحسب المصدر، لا تُحفظ البيانات البيومتريّة على حواسيب الموظّفين في السفارات، بل تُوضَّب ضمن ملفّاتٍ مشفّرة وموقّعة إلكترونيًّا، ثمّ تُنقل إلى النظام المركزيّ عبر قنواتٍ مشفّرة وبروتوكولاتٍ آمنة.

ويؤكّد أنّ المديريّة تعتمد آليّات رقابةٍ داخليّة وخارجيّة، يشارك فيها ضبّاطٌ متخصّصون بحماية المعلومات وأمنها.

كما يحصر دور الشركات المنفّذة في كونها مزوّدًا تقنيًّا لا يملك القدرة على الاطّلاع على البيانات، أو نسخها، أو نقلها، نافيًا استخدام خدماتٍ سحابيّة، أو قدرة أيّ جهةٍ غير مخوّلة على الوصول إلى النظام.

ويضيف أنّ البيانات تخضع لتدقيقٍ دوريّ، وأنّ المعلومات البيومتريّة مصنّفة وفق أعلى درجات السرّيّة.

الدولة تطلب من مواطنيها تسليم أكثر بياناتهم ثباتًا وحساسيّة، ثمّ تكتفي بالقول إنّها آمنة من دون أن تتيح لهم التحقّق.

ما لم تُجب عنه الوزارة

يقدّم الردّ الرسميّ وصفًا تقنيًّا لنقل البيانات، لكنّه لا يحسم مسائل الحوكمة والمحاسبة. فالقول إنّ الوزير "اطّلع" على القرار لا يبيّن ما إذا كان هناك قرارٌ وزاريّ معلّل ومنشور، أم أنّ المسألة بقيت في إطار إجراءٍ اتّخذه الأمن العام ووافق عليه الوزير.

كذلك، فإنّ الحديث عن رقابةٍ داخليّة وخارجيّة لا يسمّي الجهة الخارجيّة، ولا يوضّح ما إذا كانت مستقلّة عن المديريّة، ولا ينشر تقاريرها أو نتائج تدقيقها.

كما لم تسمِّ الوزارة الشركات المنفّذة، ولم تحدّد صلاحيّاتها التعاقديّة، ولا المتعهّدين الفرعيّين، ولا مَن يملك الشيفرة المصدريّة ومفاتيح التشفير، ولا ما إذا كانت الصيانة تسمح بالوصول عن بُعد.

وبقيت الكلفة بلا جواب: كم يكلّف الدفتر؟ وكم تتقاضى الشركة؟ وكم يدخل إلى الخزينة؟ ولماذا يدفع صاحب جوازٍ ساري الصلاحيّة رسمًا جديدًا؟

المسؤوليّة إذا تسرّبت البصمات

المسؤول عن جمع البيانات وحمايتها، والمطالبة بالتعويض.
أمّا جزائيًّا، فتتعلّق المسؤوليّة بالشخص الذي نفّذ التسريب أو تسبّب به، وبما إذا كان الفعل متعمّدًا أو ناتجًا عن إهمال.

> **لكنّ المسارين يصطدمان، وفق المحامي، بغياب فلسفةٍ فعليّة لجبر الضرر في لبنان. فلا توجد آليّةٌ سريعة لإبلاغ الشخص بتسرّب بياناته، أو تعويضه، أو تحديد الإجراءات التي يجب أن تتّخذها الدولة بعد الاختراق.**

ويشير إلى أنّ سرّيّة التحقيقات محميّة قانونًا، ومع ذلك تُسرَّب محاضر وتفاصيل إلى وسائل الإعلام من دون أن تُفتح تحقيقاتٌ جدّيّة في مصدر التسريب.
فإذا كانت الدولة عاجزةً عن ضبط تسريب ملفّ قضائيّ، فكيف ستتعامل مع اختراق قاعدةٍ تضمّ ملايين البصمات وصور الوجوه؟

مَن المستفيد؟

تستفيد الدولة أمنيًّا من توحيد الجوازات، وإغلاق النموذج القديم، وتقليل إمكان استخدام وثيقةٍ أصليّة بهويّة مزوّرة. وتستفيد الخزينة من الرسوم، كما تستفيد الشركات المتعاقدة من الطباعة، والصيانة، والتوسعة التقنيّة.
لكنّ تحديد المستفيد الماليّ الحقيقيّ يحتاج إلى نشر العقود والأرقام، لا إلى الاستنتاج. فمن دون معرفة كلفة إنتاج الجواز، وتوزيع الإيرادات، ومدّة العقد، لا يمكن الفصل بين الرسم الذي يمثّل كلفة خدمةٍ عامّة، والرسم الذي يتحوّل إلى موردٍ ماليّ غير خاضع لرقابةٍ كافية.

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

الوثيقة الجديدة والضمانات القديمة

ليس الجواز البيومتريّ هو المشكلة في ذاته. فهو أكثر أمانًا من النموذج القديم، ويحدّ من بعض أشكال التزوير. المشكلة أن تُبنى منظومةٌ بهذه الحساسيّة في ظلّ عقدٍ غير منشور، ورقابةٍ غير مستقلّة، وقانونٍ غير كافٍ، وتاريخٍ طويل من تسرّب البيانات من دون محاسبة.

عند نهاية الطابور، سيضع المواطن أصابعه على الجهاز، وينظر إلى العدسة، ويدفع الرسم. وبعد أيّام أو أسابيع، سيحصل على جوازٍ أحدث وأصعب تزويرًا وأقرب إلى المعايير الحديثة. لكنّه لن يحصل، في المقابل، على إجابةٍ مكتوبة عمّن يملك حقّ البحث في بصماته، ولا عن مدّة الاحتفاظ بها، ولا عن الجهة التي ستُخطره إذا تسرّبت، ولا عن التعويض الذي يستحقّه إذا استُخدمت خارج غايتها.

الدولة تطلب من مواطنيها تسليم أكثر بياناتهم ثباتًا وحساسيّة، ثمّ تكتفي بالقول إنّها آمنة من دون أن تتيح لهم التحقّق. أبطل لبنان جوازاتٍ سارية بحجّة الأمن، لكنّه لم يقدّم بعد الضمانات التي تجعل أمن الوثيقة متلازمًا مع أمن صاحبها. وبين قرارٍ غير معلّل بالكامل، وعقدٍ غير منشور، ورقابةٍ تدور داخل المؤسّسة نفسها، يبقى المواطن في الطابور الثالث، يحمل وثيقةً قالت له الدولة بالأمس إنّها صالحة، وتقول له اليوم إنّ عليه شراءها مرّةً أخرى.

وبين الوثيقتين، تظلّ بصمته الشيء الوحيد الذي لا يستطيع استبداله.

الأكثر قراءة

×

2 واشنطن والحرب الكبرى: أين العرب في صراع إيران-تركيا-إسرائيل؟

3 سحب السلاح والتحقق الدولي: هل تخرج تركيا الصواريخ إلى إيران؟

4 التشكيلات القضائية: إعادة تقييم الأسماء في مهلة الأسبوعين

إعلان

تابعنا عبر مواقع التواصل الإجتماعي

المدن
جريدة إلكترونية مستقلة .. وفي رواية أخرى

إشترك في النشرة الإخبارية ليصلك كل جديد

اشترك معنا في نشرة المدن الدورية لتبقى على اتصال دائم بالحدث

أدخل بريدك الإلكتروني

اشترك الآن

إعلان

جريدة "المدن" الإلكترونية جريدة إلكترونية مستقلة مقرها بيروت تمثل التيار المدني اللبناني والعربي

روابط سريعة

معلومات

النشرة البريدية

خطوة بسيطة وتكون من المطلعين على الخبر في لحظة ظهوره

أدخل بريدك الإلكتروني

اشترك

© جميع الحقوق محفوظة لموقع المدن 2026 محتويات هذه الجريدة محمية تحت رخصة المشاع الإبداعي